UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
-*v.*-	:	24 Cr. 424 (JGK)
HDR GLOBAL TRADING LIMITED, a/k/a/ "BitMEX,"	:	
Defendant.	:	

THE GOVERNMENT'S SUPPLEMENTAL SENTENCING MEMORANDUM

DAMIAN WILLIAMS
United States Attorney
Southern District of New York

Jessica Greenwood
Thane Rehn
Assistant United States Attorneys
Southern District of New York
- *Of Counsel* -

TABLE OF CONTENTS

The Government respectfully submits this supplemental sentencing memorandum following the *Fatico* hearing held in this matter on December 3, 2024 (the "*Fatico* hearing") and in advance of the sentencing of HDR Global Trading Limited, a/k/a "BitMEX" (the "Company" or "BitMEX") presently scheduled for January 15, 2024. The Government incorporates by reference its prior sentencing memorandum and assumes familiarity with the factual and procedural background set forth therein. (*See generally* Dkt. 18 ("Gov't Sentencing Mem.")).

PRELIMINARY STATEMENT

As set forth below, the exhibits and testimony offered at the *Fatico* hearing support a finding by a preponderance of the evidence that BitMEX earned at least $155 million in revenue attributable to U.S. sources during the relevant period of September 1, 2015, through September 30, 2020 (the "Relevant Period"). Using this U.S. revenue as the Company's gain from the offense, and in light of the remaining Guidelines calculations and Section 3553(a) factors discussed below, the Government posits that a total fine of $417 million is warranted in this case. This fine is at the middle of the Government's calculation of the Guidelines range of $293 to $541 million (the "Guidelines Range"). Notably, even if the Court were to resolve certain Guidelines disputes in the Company's favor (specifically, as to application of a 200-employee enhancement and acceptance of responsibility), the Government's proposed fine of $417 million would still be a Guidelines fine, at the top of the defense-favorable Guidelines range.

DISCUSSION

A Reasonable Estimate of BitMEX's Gain From the Offense is $155 Million

Based on the evidence presented at the *Fatico* hearing, the findings in the PSR, and the exhibits submitted in connection with the sentencing, the Government has satisfied its burden to establish by a preponderance of the evidence that the Company earned at least $155 million in

revenue from U.S. sources, based on a conservative calculation that at least 11.49% of BitMEX's revenues during the Relevant Period are reasonably attributable to U.S. sources.

To reach this conclusion, the Government: (1) identified the total value of Bitcoin deposited to BitMEX customer accounts during the Relevant Period; (2) identified the total value of Bitcoin deposits attributable to United States customers; and (3) divided the value of the United States customer deposits by the total number of deposits to calculate the percentage of overall Bitcoin deposits to BitMEX during the Relevant Period that came from known U.S. sources. These steps—and why BitMEX's challenges to them should be rejected—are described below. Thereafter, the Government will explain how its conclusion that BitMEX had at least 11.49% U.S.-source revenue during the Relevant Period is consistent with other, non-revenue data maintained by the Company, and how the Government's estimate makes numerous conservative assumptions in favor of the Company, which suggest that the actual amount of U.S.-source revenue is likely significantly higher.

A. The Government's Methodology for Calculating U.S.-Source Revenue is Reasonable and Appropriate

As set forth in further detail in the Government's original sentencing memorandum, a reasonable and conservative approach for calculating gain from this offense is to determine the revenue attributable to U.S. users of BitMEX during the Relevant Period. (*See, e.g.*, Gov't Sentencing Mem. at 10-11). Also as noted previously, the total revenue earned by BitMEX during the Relevant Period was $1.355 billion. (*See id.* at 9, 12; PSR ¶ 21).

Here, the available data produced by BitMEX does not include information that would allow the Court to directly calculate the percentage of BitMEX's total revenue attributable to its U.S. users. At base, this lack of data exists because—in willful violation of U.S. law—BitMEX failed to have any meaningful know-your-customer ("KYC") program until well after the Relevant

Period and thus did not reliably create or keep records of the identity or location of its users. (*See e.g.*, *Fatico* Tr. at 111:10-13 (testimony of defense analyst, acknowledging that BitMEX "KYC" spreadsheets to which he was given access post-dated the period covered by the relevant Gemini and Coinbase returns); *see also* Ex. B to Defense Decl. of Allan Scott Lindsay (consisting of 382 pages of partial KYC information collected by BitMEX with earliest entry of August 26, 2020)). Indeed, that deliberate failure to have a KYC program is the conduct for which the Company has pleaded guilty in this case. (Plea Tr. at 23-24). This point cannot be overstated: neither the Government nor BitMEX can use BitMEX's internal records to calculate, at least not directly, the gain derived from the offense because the Company intentionally violated U.S. law by failing to create and keep the records needed to conduct such a calculation. Even more, the Company advertised its own lack of KYC in attracting customers to register with the platform, boasting that "Sign up takes less than 30 seconds and requires *no personal information*." (*See, e.g.*, GX 31 (Sept. 15, 2015 screenshot of the BitMEX.com homepage (emphasis added)); GX 28 (September 2015 BitMEX blog post by Samuel Reed boasting that "BitMEX is one of a few Bitcoin services that does not request advanced verification from its users. Many of our users choose to remain anonymous for personal reasons, and *we respect that*.") (emphasis added)). The Company's willful failure to conduct KYC of its customers forms the gravamen of the offense conduct and cannot and should not be used by the Company as a basis to avoid the liability it faces for that conduct. Under these circumstances, it is reasonable and appropriate to approximate the revenue that BitMEX obtained from its U.S. customers through alternative data points that are available to the Court. As demonstrated below, the Government's methodology for doing so is reasonable, is supported by reasonable (indeed conservative) assumptions, and thus is more than sufficient to meet its burden to establish gain by a preponderance of the evidence.

To reasonably estimate the U.S. portion of BitMEX's overall revenue, the Government thus calculated the percentage of overall Bitcoin deposits made to BitMEX customer accounts during the Relevant Period that came from U.S. sources that the Government could identify based on other sources of information, including U.S. customers of other cryptocurrency exchanges and known U.S. crypto trading firms. To ensure a conservative estimate, the Government has also reduced this total amount of U.S.-source deposits to exclude any deposits made to BitMEX accounts that did not (according to the Company's representations) engage in actual trading activity.

This methodology—which uses the value of U.S.-source Bitcoin deposits made to accounts that engaged in actual trading as a proxy for U.S.-source revenue—is appropriate to estimate BitMEX revenue not only because of the lack of data described above, but because of the Company's business model. Specifically, during the Relevant Period, BitMEX operated as a trading platform that accepted customer deposits solely in the form of Bitcoin. (*See, e.g.*, GX 31 (Sept. 15, 2015 screenshot of the BitMEX.com homepage describing BitMEX as a "derivatives exchange" on which "All contracts are bought and paid out in Bitcoin"); GX 32 (September 30, 2020 screenshot of the BitMEX.com homepage describing BitMEX as a "crypto-products trading platform" on which "All contracts are bought and paid out in Bitcoin")). As such, Bitcoin deposits were used to fund BitMEX customer accounts that could be used to engage in trading on BitMEX that would, in turn, earn the Company revenue in the form of trading fees. Moreover, BitMEX was a margin trading platform, meaning that the permitted size of customers' trades—and the corresponding amount of fees on those trades earned by BitMEX—were directly proportional to the amount of Bitcoin that customers deposited into their accounts. Although users could deposit Bitcoin to BitMEX without actually trading—and thus without actually generating trading revenue

to the Company—the Government's estimates of U.S. deposits only include deposits made to accounts that were in fact used for trading purposes. Accordingly, it is appropriate on an aggregate level to assume that the percentage of total deposits made to U.S. trading accounts roughly correlate to the percentage of BitMEX revenues earned on those deposits.

B. Identifying the Total Amount of Bitcoin Deposits to BitMEX Customer Accounts During the Relevant Period

To identify the total value of Bitcoin deposits to BitMEX customer accounts during the Relevant Period, FBI Special Agent Alexander Vasiliades testified that he first accessed the BitMEX exchange page using a subscription-based blockchain analysis tool called TRM. (*See Fatico* Tr. at 21:4-22). After searching for the BitMEX exchange page within TRM, Special Agent Vasiliades testified that he then applied a date filter of September 1, 2015 through September 30, 2020, to reflect deposits in the Relevant Period. (*See id.* at 22:22-8). Based on that date filter, TRM identified incoming transfers to BitMEX totaling approximately $18.685 billion worth of Bitcoin. (*See id.* at 23:1-14; GX 35 at 6 (summary slide showing date-filtered TRM dashboard)).

There is no apparent dispute by the Company that TRM accurately attributed $18.685 billion worth of Bitcoin deposits to BitMEX-affiliated wallets during the Relevant Period. Indeed, the Company uses this same deposit total in its *Fatico* exhibits. (*See, e.g.*, DX 7 (defense summary slides)). Even if this figure were in dispute, the testimony establishes the reliability of this and similar TRM data. Special Agent Vasiliades testified that TRM is a subscription-based service that he regularly uses in FBI investigations and that data he has previously obtained from TRM—such as TRM's attribution of otherwise anonymous blockchain transfers to particular senders and recipients—has proven reliable and consistent with data he obtained from independent sources. (*See Fatico* Tr. at 21:10-13, 22:2-21 (direct examination) and 58:25-59:11 (cross examination)). As noted with respect to U.S.-source deposits below, the reliability of the data that Special Agent

Vasiliades obtained from TRM is further corroborated by a comparison of such data to BitMEX's own data for the same transfers identified by TRM. (*See infra* (comparing TRM attribution of Alameda, Cumberland, Galaxy, and Genesis transactions to BitMEX internal data)).

Although Special Agent Vasiliades could not testify to the specific proprietary methods used by TRM to attribute blockchain transactions to particular senders or recipients, the evidence makes clear that identifying transfers to and from BitMEX-affiliated wallets, including its customer wallets, would be a relatively straightforward exercise given BitMEX's use of vanity wallet addresses. Specifically, during the Relevant Period, BitMEX used vanity wallet addresses beginning with the prefix "3BMEX" to accept Bitcoin from its customers. (*See, e.g.*, GX 26 (October 2023 post to BitMEX's blog announcing that BitMEX would "reissue all customer Bitcoin deposit addresses . . . without our historical 'vanity' address prefix (3BMEX, bc1qmex)")). Accordingly, identifying transfers to BitMEX customer wallets (as well as certain non-customer wallets, as discussed below) would be as simple as searching public blockchain data for transfers to and from wallet addresses beginning with the prefix "3BMEX." (*See, e.g.*, GX 11 and GX 16 (transaction data produced by Coinbase and Gemini respectively, reflecting hundreds of thousands of transfers to "3BMEX" wallet addresses from U.S. customers of those exchanges); *see also* DX 1 and 2 (defense exhibit consisting of a side-by-side comparison of the Gemini and Coinbase transaction data against matching BitMEX data for those "3BMEX" transactions)). All of the foregoing demonstrates that TRM's attribution of $18.685 billion in total Bitcoin deposits to BitMEX-affiliated wallets is reliable.

Having used TRM to identify the total dollar value of Bitcoin deposits made to all BitMEX-affiliated wallet addresses during the Relevant Period, Special Agent Vasiliades then reduced that overall total by the value of Bitcoin deposited to two accounts used by BitMEX for internal, non-

customer purposes. Specifically, in advance of the *Fatico* hearing, defense counsel produced an affidavit of a corporate representative that identified two particular BitMEX accounts (the "BitMEX Corporate Accounts") as non-customer, "proprietary accounts that were used by the Company for internal treasury management." (*See* Def. Decl. of Alan Scott Lindsay ¶ 11 (identifying relevant accounts under the ID numbers 619706 and 1115489 and the registered email addresses dickman.chiu+transfer@bitmex.com and dickman@shineeffort.hk, respectively); GX 35 at 7 (summary slide excerpting that declaration)). Using the wallet addresses associated with the BitMEX Corporate Accounts—which the Company produced as part of its *Fatico* materials, along with other BitMEX account data for relevant Bitcoin transactions—the Government instructed Special Agent Vasiliades to identify all deposits made to the BitMEX Corporate Accounts and to exclude those deposits from the $18.685 billion total in Bitcoin transferred to BitMEX-affiliated wallets during the Relevant Period. (*See Fatico* Tr. at 24:5-14). Special Agent Vasiliades identified a total of $211.634 million worth of deposits to the BitMEX Corporate Accounts. (*See id.* at 24:15-18; GX 35 at 7 (summary slide)). Special Agent Vasiliades then calculated an adjusted total of $18.472 billion in Bitcoin deposits made to BitMEX-affiliated wallets used for customer accounts during the Relevant Period. (*See Fatico* Tr. at 24:21-25:1; GX 35 at 8 (summary slide reflecting adjusted total)).

In its exhibits and witness testimony, the Company does not dispute that the total value of Bitcoin deposits to the BitMEX Corporate Accounts during the Relevant Period was $211.634 million and, as noted above, does not dispute that the total value of Bitcoin deposits to all BitMEX accounts during the Relevant Period was $18.685 billion. However, the Company made no effort to exclude deposits to the BitMEX Corporate Accounts ($211.634 million) from the total value of Bitcoin transfers to BitMEX during the Relevant Period ($18.685 billion)—despite affirmatively

identifying the BitMEX Corporate Accounts as non-customer accounts. Instead, the Company only excluded deposits to the BitMEX Corporate Accounts from its analysis of *U.S.-source* customer deposits. (*Compare* DX 7 at 5 (excluding deposits to BitMEX business account from calculation of U.S. customer deposits), *with* DX 7 at 17 (noting that Company is including deposits to the BitMEX Corporate Accounts in its number for total deposits)). In other words, the Company excluded the deposits to the BitMEX Corporate Accounts *only* from the numerator of its equation, *not* the denominator. Given that the relevant inquiry is the percentage of deposits that were made to customer accounts, which could be used to generate trading revenues, deposits to the BitMEX Corporate Accounts should be excluded from the calculation entirely. The Government's methodology is consistent in that it excludes these deposits from both the numerator and the denominator. By contrast, the Company's calculation of the percentage of customer deposits attributable to the U.S. is artificially reduced due to its flawed methodology.

Based on all of the foregoing, the total of Bitcoin deposits from all sources during the Relevant Period, excluding deposits to known non-customer accounts, was $18.472 billion.

C. Identifying U.S.-Source Deposits to BitMEX Customer Accounts During the Relevant Period

Having calculated a total of $18.472 billion in Bitcoin deposits to BitMEX customer accounts during the Relevant Period, the Government next identified what portion of those overall deposits originated from U.S. sources that it could identify based on information available to it. These U.S.-source deposits fall into two broad categories: (1) known and extrapolated deposits by U.S. users of U.S.-based exchanges Coinbase and Gemini, which amount to approximately $1.201 billion worth of deposits; and (2) deposits by U.S. trading firms, which amount to approximately

$922 million. Thus, the total amount of U.S. deposits is approximately $2.123 billion.[1] The resulting percentage of total BitMEX deposits attributable to U.S. users is $2.123/$18.472 = **11.49%**. Applied to Bitmex's total revenue of $1.355 billion, the resulting revenue attributable to U.S. customers is slightly more than **$155 million**. The evidence and reasoning behind these calculations is set forth in detail below.

1. Actual and Extrapolated Deposits by U.S. Users of Coinbase and Gemini

First, the Government calculated a total of $1.22 billion in documented and extrapolated transfers from U.S. users of Coinbase and Gemini to BitMEX during the Relevant Period, as reflected in the "Documented Transfers" and "Extrapolated Transfers" subtotals below:

Coinbase and Gemini Data (GX 35 at 9):

Documented Transfers from U.S. Coinbase Users, Sep 2015-July 2020:	$676.274
Extrapolated Transfers from U.S. Coinbase Users, Aug 2020-Sep 2020	$33.973
Documented Transfers from U.S. Gemini Users, Sep 2015-March 2020:	$357.428
Extrapolated Transfers from U.S. Gemini Users, Apr 2020-Sep 2020:	$151.267

Beginning with Documented Transfers, Special Agent Vasiliades testified that he arrived at these totals by simply adding up all of the outgoing transactions reflected in subpoena returns produced by Coinbase and Gemini, which showed transfers from U.S. KYC'd customers of those exchanges to "3BMEX" wallet addresses during the bulk of the Relevant Period. (*See Fatico* Tr.

[1] At the *Fatico* hearing, the Government's witness presented a number of $2.141 billion and a resulting percentage of 11.6%. (GX 35 at 10). As discussed below, the Government is removing U.S. deposits into non-trading accounts, resulting in this slightly lower number.

at 26:4-24) (testifying that he "added the amounts" produced by KYC'd U.S. users of Coinbase and Gemini); *see also* GX 8 and 14 (subpoenas issued to Coinbase and Gemini requesting KYC and transaction data for all customers who transacted with "3BMEX" wallet addresses); GX 11 and 16 (transaction data produced by Coinbase and Gemini)). The Company's own exhibits—which include a side-by-side comparison of the Coinbase and Gemini data to BitMEX's internal records—confirm that these transactions identified by Coinbase and Gemini were in fact sent to BitMEX customer accounts. (*See* DX 1 and 2).

The Documented Transfers are based on data that ends before the end of the Relevant Period, because they were obtained through grand jury subpoenas issued during the Relevant Period. Specifically, Coinbase produced data only through July 2020, while Gemini produced data only through March 2020. (*See* GX 35 at 9). Accordingly, in order to reasonably estimate the amount of transfers that Coinbase and Gemini customers made to BitMEX *after* the available data but *before* the end of the Relevant Period, Special Agent Vasiliades testified that he used the last 6 months of available data for each exchange, calculated the monthly average of those deposits, and used that monthly average to extrapolate the total deposits made for each missing month of data. (*See Fatico* Tr. at 113:14-22). BitMEX's witness, meanwhile, acknowledged that there is no reason to believe that U.S. customers of Coinbase and Gemini abruptly stopped making transfers to BitMEX after July 2020 (the end of the Coinbase data) or March 2020 (the end of the Gemini data). Despite that concession, the defense witness made no attempt to estimate the amount of those ongoing transfers and instead simply zeroed out those totals from his calculation. (*See Fatico* Tr. at 114:16-23). The defense witness even acknowledged that his estimates are wrong if the Coinbase and Gemini deposits had continued in line with their previous activity. (*Id.*

at 115:20-22). That method should be rejected in favor of the extrapolation used by the Government, which is based on a reasonable inference.

The Company has argued for two additional categories of exclusions from the above totals.[2] The Government agrees with the first but disagrees with the second.

First, the Company argues that a total of $18.394 million (specifically, $1.84 million in Coinbase transfers, and $16.554 million in Gemini transfers) should be reduced from the Documented Transfers because those deposits were made into BitMEX accounts that did not actually engage in trading activity. (*See* GX 7 at 3, 4). The Government agrees that these deposits should be removed because non-trading accounts would not generate revenue for BitMEX. The Government notes, however, that BitMEX's witness acknowledged that he made *no attempt* to similarly exclude all deposits to BitMEX accounts with no trading history from the denominator of the relevant equation. (*See, e.g.*, *Fatico* Tr. at 101:16-23 (cross-examination testimony of defense witness)). The effect of removing deposits to non-trading accounts from the U.S. deposits, while keeping such deposits in the overall total amount of deposits, is to artificially reduce the percentage attributable to U.S. customers. And because the Company has not identified the total number of deposits to non-trading accounts, there is no way to say how significant this effect is. Nonetheless, the Government is willing to accept BitMEX's request to exclude deposits made to accounts without trading history from the U.S. deposits. Having removed those deposits, the revised total of Documented Transfers from U.S. Users of Coinbase and Gemini is $1.201 billion.

Second, the Company argues that the Documented Transfers should be reduced by a total of $284.5 million (specifically, $183.062 million in Coinbase transfers, and $101.424 million in

[2] The defense's summary slides also include line items for "Deposits missing from Coinbase KYC data" and "Deposits missing from Gemini KYC Data." (*See* DX 7 at 3-4). However, as clarified at the *Fatico* hearing, those amounts have already been excluded from the Government's totals.

Gemini transfers) because—according to limited BitMEX KYC data and a BitMEX corporate declaration—the Company asserts that those deposits were made into BitMEX accounts that were "KYC'd to non-U.S." persons or entities. (*See* DX 7 at 2, 3).

Given the offense conduct at issue in this case, that argument is particularly unpersuasive for two reasons. First, while Coinbase and Gemini in fact collected KYC data from their customers during the Relevant Period—as made clear by the hundreds of thousands of transactions that they identified between U.S. KYC'd customers of those exchanges and "3BMEX" wallet addresses—BitMEX by contrast has pled guilty *in this case* to its failure to maintain a BSA-compliant KYC program during the Relevant Period. Even after the charged time period, BitMEX has never implemented a KYC program that is compliant with U.S. law, and so the contemporaneous KYC records from Coinbase and Gemini are significantly more reliable than whatever processes BitMEX used to "KYC" these customers.

Second, Coinbase and Gemini performed their KYC at the time that customers of those exchanges transacted with BitMEX. The only KYC data that BitMEX has relied upon in challenging the Documented Transfers *post-dates the relevant transactions* and almost solely was created *after* the October 2020 indictment of the Founders for the same BSA-violating conduct that formed the basis of the Company's guilty plea in this matter. (*See, e.g.*, *Fatico* Tr. at 111:10-13 (testimony of defense analyst, acknowledging that BitMEX "KYC" spreadsheets to which he was given access post-dated the period covered by the relevant Gemini and Coinbase returns); *see also* Ex. B to Defense Decl. of Allan Scott Lindsay (consisting of 382 pages of partial KYC information collected by BitMEX with earliest entry of August 26, 2020)). Thus, even if the BitMEX data were reliable (and it is not) in determining where these customers resided later in time, it would provide no reason to second-guess Coinbase and Gemini's conclusion that these

customers were U.S. persons at the time they made the BitMEX deposits at issue here. Under these circumstances, the Court should rely upon the KYC data produced by Coinbase and Gemini as a reliable indicator of the location of the individuals who made deposits to BitMEX, and should reject BitMEX's attempts to reduce this number based on non-compliant "KYC" processes it conducted months or years after the deposits in question.

As a corollary to its request to exclude deposits to accounts that purportedly "KYC'd to non-U.S." BitMEX accounts, defense counsel suggested through questioning at the *Fatico* hearing that transfers from U.S. customers of Coinbase and Gemini cannot be used as a proxy for U.S. customer deposits to BitMEX because it would be possible for U.S. Coinbase/Gemini customers to transfer Bitcoin to BitMEX accounts held by non-U.S. persons. (*See, e.g.*, *Fatico* Tr. at 125). Although it is possible in theory that U.S. customers of Coinbase and Gemini *might* make deposits to third-party accounts at BitMEX *not* held by U.S. persons, the Company failed to provide any evidence that this occurred, much less that any such transactions occurred in any substantial quantity. The evidence indicates that such transactions would be unlikely. First, the record makes clear that BitMEX was not a peer-to-peer payment system or a banking substitute but was instead a trading firm offering novel derivatives products. (*See, e.g.*, GX 29 (snapshot of BitMEX's March 2015 FAQ page describing BitMEX as "a new type of Bitcoin exchange, built for serious traders and cryptocurrency holders with liquidity and hedging needs")). Accordingly, there is every reason to believe that customers of Gemini and Coinbase—and any other exchange—who transferred funds to BitMEX were doing so for their own benefit, in order to trade the novel products available on BitMEX. A person seeking to transfer Bitcoin to another person would be expected to use a service designed for that purpose, rather than using BitMEX. Indeed, Coinbase and Gemini specifically allow their customers to transfer Bitcoin to others, so there would be no

reason for customers of these exchanges to transfer funds to BitMEX only to then transfer them to another person. Moreover, there is no reason to believe that such transfers (if they occurred at all) would have been more likely to involve U.S. persons sending money to non-U.S. persons rather than vice versa, such that they would reduce the overall percentage of U.S. customer deposits. Particularly in light of the multiple conservative assumptions that have been made in the Company's favor, as discussed further below, and given the unavailability of contrary data caused by the Company's own failure to collect and maintain KYC records, it is reasonable to conclude that transfers to BitMEX by U.S. customers of Gemini and Coinbase are reasonably treated as U.S. customer deposits.

Based on all of the foregoing, the Government submits that a total of $1.201 billion—reflecting the adjusted total of Documented and Extrapolated Transfers from U.S. Users of Coinbase and Gemini to accounts used for trading on BitMEX—should be included in the total of U.S.-source revenues to BitMEX during the Relevant Period.

2. Deposits by Known U.S. Trading Firms

The total of U.S.-source deposits identified by the Government also includes deposits from certain crypto trading firms that were based in and primarily operated in the United States during the Relevant Period. The deposits from these companies add up to approximately $922 million (consisting of a total of approximately $469.261 million in deposits from Alameda, Cumberland, Genesis, and Galaxy, and a total of $452.480 million in "Additional U.S. Entity Deposits," which includes additional deposits from Alameda as well as other crypto firms), as shown below:

Total Deposits by Known U.S. Trading Firms (GX 35 at 9):

Blockchain Transfers from Alameda:	$263.407
Blockchain Transfers from: Cumberland:	$173.011
Blockchain Transfers from Genesis:	$15.756
Blockchain Transfers from Galaxy:	$17.087
Additional U.S. Entity Deposits:	$452.840

The first four of these line items, reflecting transfers from Alameda, Cumberland, Genesis, and Galaxy, were based on attributions to those entities from TRM. (*Fatico* Tr. 40). As described above, the testimony at the *Fatico* hearing confirms that TRM is a reliable source for this attribution. And the Court now has additional data from BitMEX that further corroborates that these deposits are attributable to the entities identified by TRM. Specifically, BitMEX's own witness analyzed these deposits and confirmed that more than 93% of these deposits were in fact attributable to the four entities identified by TRM.[3] Moreover, even for the small percentage of deposits that he disputed, BitMEX's witness offered no reason to second-guess TRM's attributions. Rather, he simply asserted with no explanation that these remaining deposits "don't appear to be" attributable to the entities identified by TRM, apparently based on some undisclosed internal attribution decision by BitMEX. (*Fatico* Tr. 78:20-21). There is no reason to credit that unexplained assertion by the defense, especially when compared with the detailed testimony

[3] *See* DX 7 at 6 (agreeing that $168.641 million out of the Government's $173.011 million are attributable to Cumberland); *id.* at 8 (agreeing that all $17.087 million of the deposits attributed by the Government to Galaxy are correct); *id.* at 10 (agreeing that $5.291 million out of $15.756 million are attributable to Genesis); *id.* at 12 (agreeing that $246.611 million out of $263.407 million are attributable to Alameda). In total, then, BitMEX admits that around $437 out of the $469 million attributed to these entities by the Government, or 93%, are attributable to the entities claimed.

regarding the reliability of TRM's attributions. Thus, the Court should credit all the attributions made by TRM or, at a minimum, credit that the 93% of these attributions that are undisputed are correct.

Subtotals for "Additional U.S. Entity Deposits" (GX 92):

Jane Street	$33,455,086.95
Tower Research	$53,234.94
Akuna Capital	$13,600,026.82
Profluent	$74,380,094.37
CMT	$10,014,834.73
Deeter Investment	$565,511.02
Merlin Capital	$82,852.92
Pier Asset Management	$495,522.35
Additional Alameda	$109,452,280.19
Phoenix Nest Invest	$224,036.54
Alt Point Capital	$6,245.94
Mosaic Exchange	$137,180.81
Jump Trading	$26,768,106.74
Circle	$183,579,994.21
Hudson River Trading	$24,561.06
	$452,839,569.59

These additional deposits do not depend on TRM attributions. Instead, they were drawn from data produced by the Company that allowed the Government to identify unique BitMEX deposit addresses associated with the BitMEX accounts for these particular U.S.-based entities. BitMEX accepts all of these "Additional U.S. Entity" attributions as accurate, with the exception of the nominal amount attributable to Hudson River Trading, which is immaterial to the overall number. (DX 7 at 13).

The Company does not dispute that five of these entities and $75 million of these deposits are attributable to the United States. (DX 7 at 14 (acknowledging that Profluent, Deeter Investment, Merlin Capital, Phoenix Nest Invest, and Pier Asset Management were affiliated with the U.S. in BitMEX's internal user table)). Thus, the dispute between the parties relates to approximately $847 million in deposits, of which almost all comes from just nine U.S.-based firms: Akuna Capital, Alameda Research, Circle, CMT, Cumberland DRW, Genesis, Galaxy Digital, Jane Street, and Jump Trading. These nine firms account for over $846 million in deposits.

The Court can easily conclude that seven of these nine firms were based in the United States because Akuna Capital, Alameda Research, Circle, CMT, Galaxy Digital, Jane Street, and Jump Trading all self-identified as U.S. trading firms when registering with Coinbase and using Coinbase's KYC procedures. (GX 9 at lines 12795, 7902, 7896, 16847, 4776, 9998, and 13637). Collectively, those seven firms alone account for around $658 million in deposits to BitMEX. As discussed above, the Court should rely on Coinbase's KYC procedures and reject any BitMEX documentation that purports to be to the contrary. Coinbase was a licensed U.S. money services business, and its KYC procedures are more reliable than the non-compliant procedures that BitMEX used, which are the subject of its offense conduct in this very case, and which for the reasons described below do not withstand even mild scrutiny.

The two remaining firms that do not appear in the Coinbase returns, Cumberland DRW and Genesis, are also plainly United States firms. Cumberland DRW was recently the subject of a SEC action in which it was identified as a Chicago-based entity. (GX 93). Moreover, Arthur Hayes described Cumberland as a U.S. entity in a 2014 email (GX 1), while BitMEX employees met with Cumberland traders in Chicago in July 2018 to discuss Cumberland's trading on BitMEX. (GX 3 at 5; GX 4). In preparing for that meeting, Greg Dwyer described Cumberland DRW as a

one of BitMEX's "clients" in Chicago in a message to Arthur Hayes. (GX 76 at 4). Similarly, the evidence shows that Genesis is a U.S. entity. Hayes met with Genesis in New York (GX 1), and the Company itself admits that it did not receive any onboarding documentation from Genesis and that at least a portion of the Genesis deposits should be attributed to the United States. (DX 7 at 10, 16).

The Company does not appear to seriously contest that these nine crypto firms are U.S.-based and that they traded from within the United States. Indeed, BitMEX's own witness acknowledged that he had no reason to believe that these firms were headquartered elsewhere or conducted any significant amount of trading elsewhere. (*Fatico* Tr. 122:12-17). Rather, BitMEX argues that these trading firms should not be included because they created offshore shell entities that BitMEX then listed as the nominal owners of their BitMEX trading accounts. (*See, e.g.*, *Fatico* Tr. at 119:5-18 (testimony of defense witness that he attributed Cumberland deposits to "Cayman Islands account" based on "information from BitMEX"); DX 7 at 6, 8, 11, 15 (summary slides excluding accounts purportedly "KYC'd" by BitMEX as "non-U.S. accounts" from the U.S. trading firm totals)). But the relevant question is where these companies were actually conducting their business and trading operations, because any such operations within the United States are subject to U.S. regulation regardless of whether these trading firms nominally placed their accounts in the name of offshore entities. *See* 7 U.S.C. § 6(a) (making it "unlawful for any person to offer to enter into, to enter into, to execute, to confirm the execution of, or to conduct any office or business anywhere in the United States, its territories or possessions, for the purpose of soliciting or accepting any order for, or otherwise dealing in, any transaction in, or in connection with, a contract for the purchase or sale of a commodity for future delivery," without complying with CFTC registration requirements and accompanying KYC/AML regulations). Indeed, BitMEX's

own onboarding procedures for these crypto trading firms acknowledged that it was not allowed to permit trading in the United States, as it asked the companies to "attest" that no such trading was occurring.

Incredibly, despite the clear evidence that these firms were in fact trading from within the United States, BitMEX now seeks to use these sham "attestations" to remove these companies' trading activity from its gain from the offense. That argument should be rejected. First, the purpose of the Guidelines calculation is to calculate the total amount of revenue from U.S. sources, not to determine whether the company knew of each individual U.S. customer that was trading on its platform. The Company's offense was to have a non-compliant KYC procedure, which by definition means that it would not necessarily be aware of all of its U.S. clients. By pleading guilty, the Company has admitted that it operated in the United States and should have conducted legally-required KYC. If it had done so, it would have concluded that these firms were in fact U.S.-based, as evidenced by the fact that Coinbase did exactly that. In essence, the Company is now attempting to use its own offense conduct—its failure to have proper KYC for these trading firms—to minimize its responsibility for this very offense.

Second, even if the Government were required to show that BitMEX knew these specific entities were trading on BitMEX from within the United States, the evidence shows that the Company was fully aware of this fact and was on notice that the "offshore" documentation submitted by these entities was a sham. For instance, on October 18, 2018, BitMEX co-founder Ben Delo explained in a chat with Greg Dwyer that the Company was not restricting United States IP addresses "due to US traders of offshore non-US corporations." (GX 6). This illustrates Delo's awareness that, even if these trading firms had submitted attestations that they were not trading

from within the United States, those attestations were inaccurate and BitMEX was deliberately choosing to continue to allow U.S.-based trading.

In addition to BitMEX's general awareness of "US traders" from these trading firms, the Company was fully aware of the U.S. status of particular trading firms. Indeed, the Company specifically advised U.S. firms to register as offshore entities while continuing to trade from within the United States. For example, in February 2018 a Jane Street trader based in New York reached out to BitMEX about setting up an account. (GX 53). A BitMEX employee advised her: "If you create an account from the U.S.A. or have plans to access the account from the U.S.A. then opening a corporate account using your UK incorporated company is the best way forward." (GX 53). Jane Street then used its UK company to create its BitMEX account and deposited tens of millions of dollars worth of Bitcoin into the account for trading purposes. (GX 92). BitMEX was fully aware that Jane Street was trading from within the United States, notwithstanding that it onboarded through a UK entity, because BitMEX executives circulated an internal list of accounts that were known to be trading from within the United States, which included Jane Street. (GX 52).

Similarly, Alameda Research, which Coinbase KYC'd as a California company, created a BitMEX account in April 2018 and was identified by BitMEX as a U.S. entity almost immediately, on May 2, 2018. (GX 39 at 45). But Alameda provided BitMEX with no documentation whatsoever for more than six months, and continued trading from within the United States throughout that time period, depositing more than $100 million into its account in its United States entity name during that time period. (*See* DX7, Slide 13, line 12 (identifying $109 million in deposits in Alameda account that never went through BitMEX onboarding process)). Finally, in December 2018, BitMEX flagged Alameda's account due to its United States activity. When that happened Alameda's owner, Sam Bankman-Fried, immediately reached out to BitMEX founder

Ben Delo about the "issues with our BitMEX account" (GX 39 at 5-6), and Delo connected Bankman-Fried to a BitMEX employee named Amy Yu, who reported that she promptly "took care of their US log-in ban." (GX 5). Bankman-Fried expressed gratitude that Yu had fixed the U.S. log-in issue so "quickly." (*Id.*). At that point in time, Yu also asked Alameda to switch its BitMEX account over to a non-U.S. entity. But her conversation with Bankman-Fried reveals that she was fully aware that this change was not connected to any actual corporate activity moving offshore. When Yu asked Bankman-Fried "what country" he would use to register the entity, he responded "easiest for us is BVI, followed by Japan—is BVI good on your end?" Yu responded that would be "fine," and Bankman-Fried said "cool let's go for BVI then!" (GX 39). The Alameda account was relisted within BitMEX as a BVI account, but there is no indication that it ever had any actual traders located in the British Virgin Islands or that BitMEX ever prevented Alameda from continuing to log in from the United States.

A similar story happened with Circle. As with Alameda, Circle submitted documents to nominally place the account in the name of an offshore entity (GX 77), but the actual certificate attached to those documents that authorized trading for the account was executed in Boston and candidly stated that the trading was being conducted by a Boston entity (GX 84). The email address for Circle's account on BitMEX, trader@circle.com, was the same email address it used for its Coinbase account, which was properly KYC'd to the United States. (*Compare* GX 84 *with* GX 9, line 7896). And BitMEX was fully aware that Circle was trading from the United States. Arthur Hayes and Greg Dwyer corresponded with Circle's head of "Trading Operations," whose email signature line identified him as having a Boston address (GX 89), and Hayes and Dwyer participated in an ongoing "BitMEX <> Circle" chat, in which they and other BitMEX employees

discussed Circle's trading activity on BitMEX with U.S.-based Circle traders, and also discussed the possibility of meeting with those Circle traders in New York and Boston. (GX 90 at 7-9).

Similar documents exist for each of these United States crypto trading firms. (*See, e.g.*, GX 2 (BitMEX founder Samuel Reed personally approving Galaxy's continued trading using New York IP address); GX 36 (Greg Dwyer meeting with Akuna's COO/CFO in Akuna's Chicago office); GX 40 (Dwyer forwarding email from Chicago-based CMT to Arthur Hayes and describing CMT as a "large trader" on BitMEX); GX 54 (Hayes meeting with traders from Jump Trading in Chicago); *see generally* GX 1-6, GX 36-73). In short, the evidence plainly shows that the nine entities identified by the Government that account for almost all the disputed deposits were United States entities, trading exclusively or primarily in the United States, and that their deposits should be included in the percentage of overall BitMEX deposits attributable to the United States.

D. A Finding that BitMEX had 11.49% U.S.-Source Revenue is Corroborated by Other, Non-Revenue Data and is Based on Conservative Assumptions that Favor the Company

As described above, the available information about BitMEX customer deposits supports a finding that at least 11.49% of all BitMEX deposits are attributable to U.S. customers engaged in trading on BitMEX, which supports an inference that at least 11.49% of BitMEX's revenue is attributable to its United States customers. There are a number of reasons to conclude that this number is a reasonable estimate and is, if anything, an underestimate of the actual gain to the Company from the offense.

First, during the first two years of the charged time period, BitMEX executive Greg Dwyer circulated quarterly "Analytics Reports" consistently showing that the United States was BitMEX's "most popular country by visits and average number of active users per day." (GX 34 at 5; *see also* GX 33 at 5). These reports were only distributed to the three BitMEX founders, and

it appears that the founders asked Dwyer to stop creating these documents after July 2017, perhaps because of how incriminating these reports were. (GX 34 at 1). In the last such report, covering the first quarter of 2017, the BitMEX executives determined that the U.S. was by far the largest source of "active users" (i.e., traders on the platform), and that the United States generated 22% of visits to BitMEX's website in the first quarter of 2017 and 16% of visits in April and May 2017. (*Id.* at 5). These numbers are broadly consistent with, and in fact higher than, the Government's estimate of the percentage of revenue attributable to U.S. users. Moreover, these numbers were calculated before most of the large U.S. crypto trading firms joined the platform, which would have likely increased these numbers.

Second, BitMEX's own internal user tables suggest that the Government's estimate is reasonable. As discussed in the PSR, the Company's user tables attributed 9.51% of trading customers to the United States. (PSR ¶ 28). In prior briefing, the Company has attempted to cast doubt on the use of that number, which led to the Court's order scheduling a *Fatico* hearing. But to the extent that the Company's user tables are not the most reliable metric of U.S. customers, that would be because these user tables are likely to underestimate the number of such users. After all, the Company publicly claimed throughout the charged time period that it did not allow U.S. users. Thus, U.S. users had an incentive to access BitMEX using a VPN or through Tor, both of which obscure the customer's location. Indeed, consistent with the Company advising U.S. institutions to open accounts using non-U.S. entities (while continuing to trade from the U.S.), the Company actively encouraged users to evade its sham controls. For instance, in September 2015, around the same time that the Company announced that U.S. users were not allowed on the platform, it also launched what it called a "hidden service" on Tor, a way of accessing BitMEX without revealing the customer's location. (GX 28). In light of this, the Company's user tables

showing nearly ten percent of customers in the United States is almost certainly an undercount. That is a further indication that the Government's estimate of 11.49% is a reasonable and conservative estimate of the true number.

Third, the Court can take note of the fact that the Company has refused to provide its own estimate or to provide the Government with access to its internal data that would allow a better estimate of trading revenue. While the Government bears the burden of proof, the Second Circuit has recognized that sentencing courts "can, and frequently do, deal with rough estimates." *United States v. Kumar*, 617 F.3d 612, 632 (2d Cir. 2010). Moreover, once the Government has "articulat[ed] a sound basis for approximation," it is appropriate for the sentencing court to inquire whether the defendant can "refute this showing." *United States v. Gushlak*, 728 F.3d 184, 202 n.15 (2d Cir. 2013). Even when the Government's proposed methodology is based simply on a witness's "estimates," the Second Circuit has affirmed a Guidelines calculation where the defendant "did not produce any evidence contradicting" those estimates. *United States v. Germosen*, 139 F.3d 120, 129 (2d Cir. 1998). Given those legal principles, it is striking that the Company has made no effort to propose any alternate methodology for calculating its gain from the offense, despite being in full possession of its own trading data and has not produced this data to the Government. For instance, at the *Fatico* hearing, defense counsel argued that there may not be a perfect correlation between customer deposits and BitMEX's trading revenue. (*Fatico* Tr. at 8). But the Company knows exactly which customer accounts the Government is attributing to the United States, and yet has never submitted any evidence to suggest that the percentage of revenue attributable to those accounts is lower than the percentage of deposits attributable to those accounts. That is a telling omission, and supports the inference that the Government's methodology of using the deposits from these accounts to estimate revenue is reasonable.

Fourth, the Government's methodology makes a number of conservative assumptions and is likely to result in an underestimate of the gain to the Company from the offense. For example, the Government's estimate is limited to U.S. customers who happened to also be customers of either Coinbase or Gemini and who funded their BitMEX accounts using their Coinbase or Gemini account. Any U.S. person who funded his account from another crypto exchange, or from a privately controlled Bitcoin wallet, is not included in the Government's estimate of U.S. users, even though such deposits are visible on the blockchain and are therefore included in the total amount of deposits to BitMEX customer accounts. Additionally, the Government only identified the BitMEX accounts of a small number of prominent U.S. crypto trading firms, despite the evidence that there were multiple others. For example, in his discussion of BitMEX's "clients" in Chicago in GX 76, Dwyer mentioned several firms that are not included in the Government's estimate, such as TT, Nomad, and Hehmeyer Trading. (GX 76 at 4). Moreover, and as described above, the Government's estimate of deposits from U.S. customers only includes deposits into accounts that were actually used for trading. But in its estimate of the total number of BitMEX deposits, the Government includes deposits to all customer accounts, even accounts that were not used for trading, which artificially inflates the denominator and reduces the percentage of U.S. deposits. Collectively, these issues mean that the Government's number is a highly conservative estimate of the true percentage of BitMEX deposits for trading that are attributable to the U.S.

CALCULATION OF THE GUIDELINES FINE

To calculate the appropriate sentence for a corporation, the United States Sentencing Guidelines ("U.S.S.G." or "Guidelines") set forth a multi-step process. First, the Court should calculate the base fine amount, which in this case is the amount of the Company's gain from the offense. U.S.S.G. § 8C2.4. Second, the Court should calculate the culpability score based on

U.S.S.G. § 8C2.5, which is used to determine the appropriate multiplier in U.S.S.G. § 8C2.6. The multiplier is multiplied by the base fine to generate a sentencing guidelines range, U.S.S.G. § 8C2.7, and the Court considers where within this range the fine should be set, U.S.S.G. § 8C2.8. Third, the Court shall then add to the fine the gain to the company, less any remedial payments the company has made, as disgorgement. U.S.S.G. § 8C2.9. Finally, because BitMEX was a closely held company, the Court "may" offset from the fine any fine amounts paid by the Founders. U.S.S.G. § 8C3.4.

A. Step One: Calculating the Gain from the Offense

The first step is to calculate the gain from the offense, which serves as the base fine level in this case pursuant to U.S.S.G. § 8C2.4(a)(1). Under the Guidelines, pecuniary gain is defined as "additional before-tax profit to the defendant resulting from the relevant conduct of the offense. Gain can result from either additional revenue or cost savings." U.S.S.G. § 8A1.2, Application Note 3(H). Thus, the question is what "additional revenue" or "cost savings" resulted from the offense conduct.

As the Government discussed in more detail in its prior sentencing submission, it would be perfectly reasonable for the Court to determine that the appropriate calculation of gain from the offense is the total amount of revenue the Company earned while operating in the United States. (*See* Gov't Sentencing Mem. at 11). BitMEX plainly conducted business in the United States throughout the charged time period. The Commodity Exchange Act applies to all entities that "conduct any office or business in the United States." 7 U.S.C. § 6. BitMEX was continuously physically present in this country and therefore was required to register with the CEA and to have a fully compliant AML and KYC program not only for its U.S. users, but for all of its users, and yet it did not implement any such program. Under a straightforward reading of the statute, a reasonable calculation of the gain from the offense is the Company's *entire* revenue from its non-

compliant ongoing operations while present in this country (*i.e.*, the Relevant Period). That calculation would result in a base offense level of $1.355 billion.

The second approach for calculating the pecuniary gain, and the one that the parties have focused on, is to base gain only on the revenue the Company earned from its U.S.-based *customers* (rather than its U.S.-based operations more broadly). As demonstrated at the *Fatico* hearing and discussed above, a conservative estimate of that number, making a number of assumptions that are favorable to the Company, is that approximately 11.49% of the Company's total revenues for the charged time period are attributable to its United States-based customers, which amounts to approximately $155 million. Although this is very likely an underestimate of the actual gain from the offense, the Government submits that it is a reasonable number for the Court to use to calculate the Guidelines range in this case.

B. Step Two: The Culpability Score and Multiplier

After determining the gain amount, the next step in the analysis is to calculate the Company's Culpability Score. Under U.S.S.G. § 8C2.5(a), the Culpability Score begins at 5.

The next step is to determine how many points to add based on the size of the corporate entity. In its prior sentencing submission, the Government argued that three points should be added pursuant to U.S.S.G. § 8C2.5(b)(3), because the Company had more than 200 employees, and Company executives participated in the offense. (*See* Gov't Sentencing Mem. at 16-17). The Company has argued that only a 2-point increase is warranted under U.S.S.G. § 8C2.5(b)(4), because it claims that it did not have more than 200 employees.

There is no dispute that the Company's "headcount" was greater than 200 during the charged time period, but that number apparently includes independent contractors. (PSR ¶ 55). The Government submits that, because the purpose of this Guideline is to calibrate the appropriate penalty to the size of the business, it is irrelevant whether a company conducts its operations

through formal employees or through independent contractors who are functionally employed by the company. *See, e.g.*, *Anthony v. Nw. Mut. Life Ins. Co.*, 130 F. Supp. 3d 644, 652 (N.D.N.Y. 2015) (Sarbanes-Oxley protections for whistleblower employees also apply to "a contractor employee [who] is functionally acting as an employee of a public company"). The bottom line is that the Company was one of the world's largest cryptocurrency exchanges during the Relevant Period, and that it had hundreds of millions of dollars in annual revenue, making a three-point enhancement appropriate. However, in the alternative, if the Court determines only to award a two-point enhancement, then it should take into account the magnitude of the Company's operations and impose a sentence on the high side of the resulting Guidelines range.

Next, the Court should consider whether to reduce the Culpability Score pursuant to U.S.S.G. § 8C2.5(g). BitMEX acknowledges that it is not entitled to a two-point reduction, but argues for a one-point reduction pursuant to § 8C2.5(g)(3). (Dkt. 15 at 17). To be sure, the Company entered a guilty plea, which "ordinarily" suffices to show acceptance of responsibility for the one-point reduction. U.S.S.G. § 8C2.5 cmt. n. 14. However, the Government submits that this is not the ordinary case.

As the Court has now seen, BitMEX has not demonstrated acceptance of responsibility in any real sense. Even after its Founders and chief executives were indicted, the Company did not admit wrongdoing but insisted that there had been no criminal conduct until after the Founders entered their guilty pleas. It then acknowledged that it had no choice but to plead guilty to the offense, but refused to engage in any serious discussion about its gain from the offense or disclose information that would enable the Government and the Court to more precisely identify the gain from the offense. In short, BitMEX did not "clearly demonstrate[] recognition and affirmative acceptance of responsibility for its criminal conduct." U.S.S.G. § 8C2.5(g). The purpose of

receiving a reduction in Culpability Score is to recognize when a corporate entity has facilitated the efficient resolution of its case and the administration of justice by affirmatively taking responsibility for the full scope of its criminal conduct. Taken by itself, the Company's guilty plea, which was an unavoidable outcome of the fact that all of its owners and top executives had already entered guilty pleas for the same conduct, does not meet that standard. Thus, the Government submits that this one-point reduction is unwarranted.

If the Court applies the 200-employee enhancement and denies the one-point reduction for acceptance of responsibility, the Company's Culpability Score is 8. Pursuant to U.S.S.G § 8C2.6, this results in a fine multiplier of 1.6 to 3.2, and (using a gain amount of $155 million, as discussed above), that multiplier leads to a base Guidelines Range fine of $248 million to $496 million. If the Court were to deny the 200-employee enhancement and/or grant the Company a one-point reduction for acceptance of responsibility, the Culpability Score would be either 7 or 6, and the multiplier and base range would be reduced accordingly. Regardless of the Culpability Score, the Guidelines Range is next adjusted to reflect disgorgement and offset; as detailed below, this step results in a net increase to the fine of $45 million.

For ease of refence, the potential range of these Culpability Scores, multipliers, and Guidelines Ranges, both before and after disgorgement and offset, as calculated below, is set forth in the following table:

Culpability Score	Multiplier	Base Guidelines Range	Net Adjustment for Disgorgement/ Offset	Total Guidelines Fine Range
8 *Assuming 200-employee enhancement and no reduction for acceptance of responsibility*	1.6 to 3.2	$248 to $496 million	Plus $45 million	$293 to $541 million
7 *Assuming no 200-employee enhancement and no reduction for acceptance of responsibility*	1.4 to 2.8	$217 to $434 million	Plus $45 million	$262 to $489 million
6 *Assuming no 200-employee enhancement and 1-level reduction for acceptance of responsibility*	1.2 to 2.4	$186 to $372 million	Plus $45 million	$231 to $417 million

Notably, the three alternative calculations set forth above include a significant amount of overlap—in other words, any fine of at least $293 million (the bottom of the Government-proposed Guidelines Range) or no more than $417 million (the top of the Guidelines range that would result from resolving disputed Guidelines issues in the defendant's favor), would be within the range of any of the above Guidelines calculations.

The next step is for the Court to determine the appropriate fine based on the sentencing factors set forth in U.S.S.G. § 8C2.8. For the reasons discussed below, the Government submits that a sentence in the middle of the Government's proposed Guidelines Range—which is also at the top of the most defense-friendly range outlined above—is warranted. The conduct was willful, it went on for a period of five years, it was perpetrated at the highest levels of the Company, and the need for deterrence is especially acute in this case. Thus, the fine should be $417 million inclusive of disgorgement and offsets, as described below.

C. Steps Three and Four: Disgorgement and Offsets

After calculating the base Guidelines range, the Guidelines instruct that the Court "shall add to the fine" the amount of gain to the organization, but should reduce this disgorgement amount by anything that has been "paid as restitution or by way of other remedial measures." U.S.S.G. § 8C2.9. Here, the gain to BitMEX is $155 million, but it has paid $80 million to settle its cases with the CFTC and FinCEN. Thus, under U.S.S.G. § 8C2.9, the Court should add $75 million to the base fine ($155 million minus $80 million).

Finally, under U.S.S.G. § 8C3.4, the Court may offset the fine to reflect the $30 million in fines already paid by each of the Founders, given that BitMEX was and remains a closely held corporation. Although this decision is discretionary with the Court, the Government does not dispute that it would be an appropriate decision to reduce the total fine by $30 million in offsets here.

The net adjustment for disgorgement and offsets is therefore $45 million ($75 million in disgorgement minus $30 million in offsets). As such, the Government posits that a total fine of $417 million—which is at the mid-point of the Government's Guidelines Range after including disgorgement/offsets and at the high point of the range if the Court agrees with BitMEX on certain Guidelines enhancements—is appropriate in this case.

A SENTENCE AT THE MIDDLE OF THE GUIDELINES RANGE IS APPROPRIATE

The Government's prior sentencing submission outlined in greater detail the reasons why the Section 3553(a) factors weigh in favor of a substantial sentence in this case. BitMEX willfully violated United States law for five years, and these willful violations were personally approved and executed at the very highest levels of the Company. The evidence presented at the *Fatico* hearing conservatively shows that the Company reaped over $155 million in gain from the offense, but even that number understates the magnitude of the offense. The Company permitted more

than $2 billion worth of deposits from United States persons. And due to its complete failure to adopt any anti-money laundering program, BitMEX permitted customers to transact anonymously with no controls, and did so despite repeated warnings from law enforcement around the world about suspicious activities on the platform. As the Government has described in prior submissions, this resulted in hundreds of millions of dollars' worth of suspicious transactions, sanctions violations, and likely money laundering. To be clear, BitMEX did not simply have an inadequate AML program. It did not implement any AML program at all, and its failure to implement an AML program meant that it was harder for law enforcement to identify criminal activity and track victim funds.

Moreover, the sentence in this case must take into account the need "to afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(B). As both parties agree, this prosecution has been closely watched in the cryptocurrency industry. Cryptocurrency exchanges are corporations that are primarily driven by the profit motive. The mere fact of a criminal conviction, without a significant financial consequence attached to that conviction, risks sending a message that willfully violating United States law is worth the risk. That is especially so where, as here, the exchange has deliberately marketed itself to United States customers for years, processing billions of dollars in transactions and pocketing over $155 million in fees from those customers. The sentencing guidelines for corporations recognize that, in circumstances like this case, the appropriate sentence must be a multiple of the gain from the offense. *See United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994) ("Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it."); *see also United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir.

2018) (citing *Heffernan*). The Government submits that a within-Guidelines sentence is sufficient, but not greater than necessary, to comply with the purposes set forth Section 3553(a).

CONCLUSION

In light of the record, the Sentencing Guidelines, and the Section 3553(a) factors, the Government respectfully submits that a sentence at the mid-point of the Guidelines Range, plus the net of disgorgement and offsets, is warranted. Accordingly, the Court should impose a total fine of $417 million.

Dated: New York, New York
December 10, 2024

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: *s/ Thane Rehn*
Jessica Greenwood
Thane Rehn
Assistant United States Attorneys
(212) 637-1090/2354